KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Exam 2012-12-14, 14.00 –19.00

This is a closed-book exam, no material (books, articles, laptops, phones, or any other electronic devices, etc.) permitted. Please answer in English if you can, only answer in Swedish if you must. Grading is according to the following preliminary point allocations. E 16–19p, D 20–22p, C 23–25p, B 26–28p, A 29–31p. Good luck!

1 Intrusion Detection. [2 points]

1a Explain the concepts of false negatives and false positives. What happens if you tune your intrusion detection system toward higher or lower sensitivity? What are the security consequences for each of these two cases?

Sample solution:
False positives means benign actions were categorized as intrusions. False negatives means an intrusion occured but was not detected. If one allows for more false positives, real intrusions are likely to be detected (more secure) but there will be many false alarms which might train the administrator to ignore them or even lead to denial of service. If one allows for more false negatives, many attacks might go undetected (less secure), but the few alarms that do go off will likely concern a real intrusion and can be taken seriously.

1b Discuss how anomaly detection and signature-based detection relate to false positives and negatives. Give an example each.

Sample solution:
Anomaly detection might have more false positives as e.g., a user coming in late in the evening might be an unusal but still legitimate behavior. Signature-based detection tends to have more false negatives as new attacks take some time to be identified and not all attacks have unambiguous signatures, e.g. a new polymorphic virus.

2 CIA. [1 point]

2a What can you do to make sure a file has not been tampered with (integrity) - name and explain two strategies for doing that.

Sample solution: Message authentication codes, hashes (with asymmetric encryption, with symmetric encryption, with secret value), digital signatures.
Each has a different way of arriving at a message digest that can be recreated at the receiver to compare and detect if anything has changed. See chapter 2 of the course book for the individual cases.

3 Secure E-Mail. [1 point]
Alice and Bob use GnuPG or something similar to send secret messages to each other. Make a diagram and explain how they can do this.

3a Who has which keys, how do they best get them?

Sample solution: Alice has her private and public key and Bob's public key Bob has his private and public key pair and Alice's public key Alice uses Bob's public key to encrypt the clear text and thus turns it into the ciphertext. She uses her private key to sign it and sends it to Bob.
Bob decrypts the ciphertext using his private key and uses Alice's public key to verify the signature. He now has the plaintext.
Alice and Bob should use certification authorities, personal meetings or several sources to exchange public keys and check for signatures.

4 Diffie-Hellman Key Exchange. [2 points]

4a Given Bob's public key Y_B, generated using the prime number q and α, a primitive root of q (same q and α as Alice used for her keys Y_A and X_A), how can Alice generate the secret key she shares with Bob?

Sample solution:
$Y_B^{X_A}$ mod q

4b What would Darth need to do to be able to read the messages between Alice and Bob?

Sample solution:
Intercept their exchange of public keys, find q and α, and mount a man-in-the-middle attack by sending a Y_{DB} to Alice and a Y_{DA} to Bob, sharing a secret with each separately. Alternatively, in theory, he could solve the discrete logarithm, but in practice he would not be able to do so.

5 Authentication. [5 points]
This summer it emerged that several million user names and passwords from LinkedIn.com were leaked by hackers and put up on a web forum. The passwords were hashed but not salted.

5a What can the hackers or anyone that downloaded the files do to get to the plaintext passwords?

Sample solution:
Mount a dictionary attack, brute-force attack, use rainbow tables.

5b What if the passwords had been salted - with the same salt for each user?

Sample solution:
There can be collisions and users that have the same password will have the same hash. If a password is found for one, then the same is done for all who have the same password.

5c What if the passwords had been salted - with a different salt for each user?

Sample solution:
No collisions, each password needs to be cracked separately.

5d What would you recommend to the LinkedIn security team to best protect user passwords, give at least 3 recommendations and reasons for them.

Sample solution:
Use a different salt for each user to avoid collisions and make rainbow tables useless, choose long enough salts for increased difficulty and long enough hashes to avoid collisions, protect access to the password file to prevent leakage in the first place, don't store passwords in plaintext anywhere to not undo the benefits from following the othe recommendations.

5e What would you recommend to LinkedIn users to best protect their passwords on the site and others, give at least 3 recommendations and reasons for them.

Sample solution:
Choose different passwords for different sites to avoid hacks from one site to affect your account on another, make them long and complicated and don't make them guessable in order to make them harder to crack, change your password from time to time.

6 Malware. [3 points]

Your friend Jonas tells you that his antivirus program subscription had run out and he didn't renew it for three months. You of course tell him that he should get a good malware detection program and check his computer. He agrees and tells you that, indeed, the (new) antivirus program found some viruses and has now cleaned them off the system.

6a Is everything alright now? Give reasons.

Sample solution:
Probably not, there could be malware that was not detected by his new antivirus program, e.g. rootkits that hide from detection.

6b What if the malware detection program Jonas used was itself malware?

Sample solution:
Not only are viruses not removed from his disk, but new malware is installed, all the while Jonas thinks that his system is secure.

6c What would you recommend Jonas to do to make reasonably sure that the malware detection program he installs is safe?

Sample solution:
Install programs from reputed providers and make sure he gets the right file by checking the hashes/MAC.

7 Buffer overflows. [3 points]

7a Make a drawing to show what a buffer overflow attack on the stack looks like. How does it work?

Sample solution:
see stack drawings in the course book. The stack grows down and buffers are filled going up. If the input exceeds the buffer size, more stack memory above will be overwritten.

7b You are given the task to maintain a program written by someone else in the C language. What can you do to make sure the program is protected against buffer overflows? Explain at least two kinds of protection you can apply as a programmer.

Sample solution:
Check input, check buffer sizes and types, use newer and safer libraries, use Stackguard or a similar tool when compiling.

7c How can an attacker not just crash a program with a buffer overflow attack but use the attack to run their own code?

Sample solution:
The attacker must first identify somehow (e.g. tracing, fuzzing tools) the buffer overflow vulnera- bility in a program. The idea is to input more data to the buffer than it is supposed to handle. By overwriting the return address in the stack frame, one can get a segmentation fault or an illegal instruction error. This happens when function returns and tries to execute instructions at the location pointed by return address. There is a very high chance that the overwritten return address would not point to a valid address inside the process address space or the instruction would be valid if the attacker used some random input, and the program would crash. To run arbitrary code attacker should put executable code in the buffer that is being overflowed and overwrite the return pointer to point to the buffer. The attacker has to guess the address of the buffer to succeed. The attacker can add NOP instructions at the beginning of the buffer, then add the executable code, and then overwritten return address. This greatly increases the chances of guessing the address, because even if the pointer does not point precisely to the beginning of the injected code but points instead to one of the NOP instructions, then NOP instructions will be executed and eventually the injected code will be executed after them.

8 Security principles. [1 point]
The IT team in your company configured the system such that it forces the users to change their password every week, keeping in line with guidelines that the password should be at least 20 characters long, consist of uppercase and lowercase letters, numbers, and special characters. The users are not allowed to reuse any password they have used before.

8a This goes against at least one major security principle. Which? And what are the security consequences of this choice?

Sample solution:
Principle of psychological acceptability. This seems to much to ask from users and they might start writing down the password on post-its under the keyboard. (Another principle is that of economy of mechanism, this uses too much effort when simpler systems would suffice.)

9 Social engineering. [2 points]
You are hired to be a security consultant and trainer called in to help KTH CSC to specifically avoid social engineering attacks.

9a What are the 3 main pieces of advice you give to the people working in the personnel (HR) and economics administration?

Sample solution:
Create a climate where it is ok to verify requests and to say no, even to what seems to be authority figures. Be aware of situations that might impair you judgment, such as flattery, helplessness, pressure, stress, etc. Follow any security policies, keep a mindset that doesn't include trusting everybody,

9b Same as above but for the people in charge of security and systems administration? (Do not repeat any advice already given above.)

Sample solution:
Create security policies for 1) how to handle requests 2) how to verify identities 3) what information to give out to whom (or never), educate and train users. Use the principle of separation of duties.

10 Consulting. [1 point]
How would you respond to the following statements? Come up with an argument for why this is or is not a good idea.

10a I am sick and tired of spam. Now I'll configure my mail system to use a white list, so that only useful mails get through.

Sample solution:
Not a good idea, unless you don't want to be contacted by anyone you haven't whitelisted yet.

10b I like it when a web service can send me my password again in a reminder e-mail. This way it's more secure as I don't have to remember so much and am thus less likely to use the same password for different sites or write them down.

Sample solution:
Not a good idea, if they can resend the password it means they store it in plaintext and any intruder can find it without having to crack it.

11 Web attacks. [2 points]
Make a diagram showing the user Ursula's desktop, the server of the webservice Webbankingservices.com and the attacker Alfred's laptop.

11a Show and explain an example of cross-site scripting. What happens at each of these machines?

Sample solution: main point: code gets executed at Ursula's and has an effect there.

11b Same for cross-site request forgery.

Sample solution: main point: the effect is on Webbankingservices.com, a request looks like it came from Ursula but was initiated by Alfred and the changes happen at Webbankingservices.com.

12 Firewalls. [2 points]
Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop computers, and laptops against networks threats.

12a A firewall at the network perimeter (i.e., where the network meets the Internet)

Sample solution:
Strength: this tackles the bulk of the traffic
Weakness: vulnerable to internal attacks; one-size-fits-all, can't have different policies for different servers/clients.

12b Firewalls on every end host machine

Sample solution:
Strength: can be adapted to the needs of each host
Weakness: many installations and configurations need to be kept up-to-date

12c All of the above: a network perimeter firewall and firewalls on every end host machine.

Sample solution:
Strength: First line of defense by the perimeter firewall plus individual firwalls provide a second line of defense. The perimeter firewall can have basic settings for all, the individual ones augment for specifics.
Weakness: maintenance and coordination effort.

13 Multi-Level Security, Mandatory Access Control. [2 points]

13a What is the meaning of the no-read-up-no-write-down policy in Bell LaPadula and what does it protect against?

Sample solution:
A subject with a given clearance cannot read objects at a higher security level and can not write to objects that have a lower security level than the subject's clearance. The protection is against leaking information from higher to lower levels.

13b Lena just started working as a lawyer. The company she joined uses a Chinese Wall system to protect their clients. Since she's new, she can access any information. Is that true? What happens once she has accessed a particular client's data?

Sample solution:
Yes, she can access any data. Once she has accessed one piece of data, that determines which data set she has access to and what the conflicts are that prevent here from accessing other data. A piece of the Chinese wall is built depending on which data she accessed first.

14 Audits. [1 point]

Name and explain the steps in the audit process.
Sample solution:
Define Goals, Identification of Risks, Identification of Controls, Design Evaluation of Controls, Operational Evaluation of Controls
see slides.

15 Denial of Service. [1 point]

How does a SYN spoofing attack work and what is its effect?
Sample solution:
TCP has a three-way handshake to set up connections. The attacker spoofs many source IP addresses and sends SYN packets to the target. The Target responds with a SYN-ACK message (or several due to timeouts), but they get sent to the fake addresses and thus are not followed by the expected ACK message. The target eventually runs out of space, keeping track of these open fake requests. Even legitimate requests cannot make it through anymore and thus service is denied.

16 Secure Hash Functions. [2 points]

You are planning to enter the next competition for a secure hashing algorithm. What are the requirements you need to fulfill? Name and explain at least 4.
Sample solution:
one-way function, collision resistance, same input needs to generate same hash output, accept variable-length input and hash to fixed-length output.